

Application Serial No. 09/665,018

REMARKS

The Applicants and the undersigned thank Examiner Colin for his time and consideration given during the telephone interview of October 4, 2005. The Applicants and the undersigned also thank the Examiner for his careful review of this application. Claims 1-20 have been rejected. Upon entry of this amendment, Claims 1-20 will remain pending in this application.

The independent claims are Claims 1, 8, and 11. Consideration of the present application is respectfully requested in light of the telephonic interview, the above amendments to the claims, and in view of the following remarks.

Summary of Telephonic Interview of October 4, 2005

The Applicants and the undersigned thank the Examiner for his time and consideration given during the telephonic interview of October 4, 2005. During this telephonic interview, a proposed amendment to the claims provided by the Applicants prior to the interview was discussed.

The Applicants' representative explained that the prior art of record does not provide any teaching of generating workstation credentials derived from a scanner conducting the vulnerability assessment of the workstation and where the workstation credentials comprise at least one of information about integrity of the workstation and a security posture of the workstation. It was explained that the prior art does not provide any teaching of comparing the workstation credentials to a workstation policy in order to grant the workstation access to one or more services available on a network server if the workstation credentials are in compliance with the workstation policy.

To emphasize that the prior art of record does not grant access to a network service for a workstation, but instead, only authenticates a user to access a service, the Applicants' representative pointed out that the amended independent claims recite that a request for credentials associated with a user is issued after a workstation is granted access to a service in order to determine if the user is authorized to access the a service available on a network server. This means that each of the independent claims require at least two authentication steps: (1) granting a physical workstation access to a service;

Application Serial No. 09/665,018

and (2) granting a user access to a service if the physical workstation is granted access to the service.

U.S. Patent Application Publication No. 2001/0034847, published in the name of Stephen E. Gaul (hereinafter, the "Gaul reference") may provide a teaching of generating workstation credentials. However, it was explained that this reference does not use these workstation credentials to grant a workstation access to a network service before a request is issued to authenticate a user to determine if a user should be permitted to access the network service.

U.S. Patent No. 6,438,600 issued in the name of Greenfield et al. (hereinafter the "Greenfield reference") describes technology that only authenticates users and not a physical workstation. In other words, the Greenfield reference like the Gaul reference does not provide any teaching of checking workstation credentials associated with the workstation (and not with the user) in order to grant a workstation access to a network service.

Similarly, the printed publication entitled, "White Paper: Secure Computing with Java: Now and the Future," that was published in 1994 and authored by Gary McGraw and owned by Sun Microsystems, Inc. (hereinafter the "McGraw publication") only describes authenticating a user to access a service and not granting a workstation access to a service irrespective of a user.

Examiner Colin indicated that he understood the Applicants' position and that he would consider it when the formal response was filed. The Applicants and the undersigned appreciate the Examiner's time and consideration given during the telephone interview of October 4, 2005.

The Applicants and the undersigned request the Examiner to review this interview summary and to approve it by writing "Interview Record OK" along with his initials and the date next to this summary in the margin as discussed in MPEP § 713.04, p. 700-202.

Claim Rejections under 35 U.S.C. §103

The Examiner rejected Claims 1-20 under 35 U.S.C. 103(a) as being unpatentable over the Gaul reference in view of the Greenfield reference and the McGraw publication.

Application Serial No. 09/665,018

The Applicants respectfully offer remarks to traverse these pending rejections. The Applicants will address each independent claim separately as the Applicants believe that each independent claim is separately patentable over the prior art of record.

Independent Claim 1

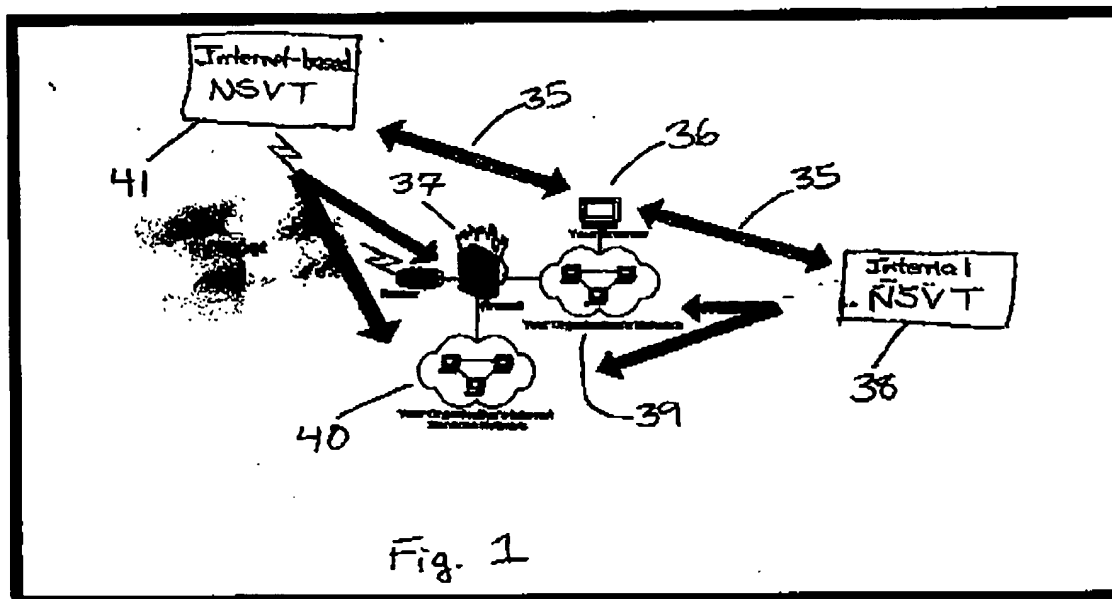
The rejection of Claim 1 is respectfully traversed. It is respectfully submitted that the Johnson and Gaul references fail to describe, teach, or suggest the combination of: (1) issuing a request for a scanner from a browser operating on the workstation to a network server via a computer network; (2) transmitting the scanner from the network server to the workstation via the computer network, the scanner installable within the browser and operative to complete a vulnerability assessment of the workstation to identify security vulnerabilities of the workstation that can compromise secure operation of the workstation on the computer network; (3) generating workstation credentials derived from the scanner conducting the vulnerability assessment of the workstation, the workstation credentials comprising at least one of information about integrity of the workstation and a security posture of the workstation; (4) comparing the workstation credentials to a workstation policy; granting the workstation access to one or more services available on the network server if the workstation credentials are in compliance with the workstation policy; and (5) if access to the one or more services available on the network server is granted to the workstation because the workstation credentials are in compliance with the workstation policy, issuing a request for credentials associated with a user; (6) receiving credentials associated with a user; (7) and determining if the user is authorized to access the one or more services available on the network server by (8) evaluating the credentials associated with the user, as recited in amended independent Claim 1.

The Gaul Reference

The Gaul reference describes a system that allows Systems Administrators and Network Managers to perform Internet security vulnerability assessments from outside of an organization's firewall 37. See Gaul reference, page 2, first column, paragraph 0016. The system of the Gaul reference allows a system administrator to use an internet

Application Serial No. 09/665,018

browser running on a client 36 to access an external Internet-based Network Security Vulnerability Testing (NSVT) application 41 and an internal Network Security Vulnerability Testing (NSVT) application 38. See Figure 1 of the Gaul reference reproduced below.



With NSVT applications 38, 41 the user running the client 36 can launch security testing against any one system or multiple systems. See Figure 1 of the Gaul reference reproduced above and page 3, first column, paragraph 0031.

The Gaul reference provides security testing or vulnerability testing of its computer system elements, but it does not use its security testing or vulnerability testing in connection with allowing a computer system element to gain access to a network or service. The Gaul reference is only concerned with random testing of its system components under control of system administrators and repairing those components if the components fail a test.

Meanwhile, the Applicants' invention generates workstation credentials that are derived from a scanner conducting a vulnerability assessment of the workstation; compares the workstation credentials to a workstation policy; the invention grants the workstation access to the network server if the workstation credentials are in compliance with the workstation policy; if access to the network server for the workstation is granted

Application Serial No. 09/665,018

because the workstation credentials are in compliance with the workstation policy, a request is issued for credentials associated with a user in order to determine if the user is authorized to access the one or more services available on the network server, as recited in amended independent Claim 1.

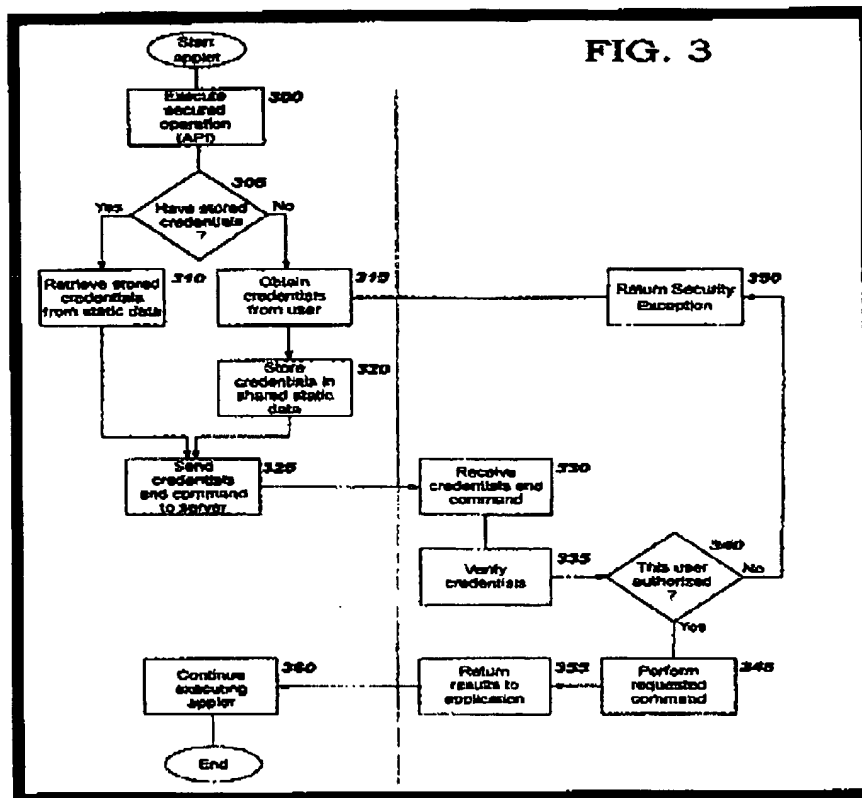
The Greenfield Reference

The Greenfield reference generally describes a computer program for securely sharing log-in credentials among trusted browser-based applications. Credentials for a user can be automatically shared only among a restricted and authorized set of trusted applications, without requiring the application developer to write code to manage the credentials. A single log-in is used to obtain the user credentials for a particular codebase, and the credentials are then reused for applications in that codebase. See Greenfield reference, Abstract.

The Examiner alleges that Figure 3 of the Greenfield reference teaches the transmitting of workstation credentials to a server. The Greenfield reference explains Figure 3 illustrates one approach that may be used to verify credentials, and involves transmitting the credentials to a server.

Block 325 in Figure 3 sends the credentials and the command (i.e. the request for a secured operation) to a server. This information is received by the server at Block 330, and verified (using application-specific processing, as previously stated) at Block 335. A test is made at Block 340 to determine whether the result of the verification process indicates that the user is authorized. If so, Block 345 performs the requested command, and Block 355 returns the result to the client machine. The applet then continues its execution, using these returned results, at Block 360. See Figure 3 of the Greenfield, reproduced below and column 8, lines 26-38.

Application Serial No. 09/665,018



While the Greenfield reference may teach transmitting “credentials” from a workstation to a server, these are credentials that are associated with a user and not ones derived from a scanner conducting a vulnerability assessment of the workstation. The Greenfield “credentials” are not workstation credentials comprising at least one of information about integrity of the workstation and a security posture of the workstation, as recited in amended independent Claim 1.

The Greenfield reference defines credentials as application-specific information (such as a user name or other identifier, a user password, etc.) that identifies the requesting user at the client machine. These credentials are compared to a previously-defined, stored set of the credentials for all authorized users. If the credentials match an entry in this stored set, then this user is an authorized user. See Greenfield reference, column 2, lines 48-55. Therefore, while the Greenfield reference teaches authenticating a user, the Greenfield reference does not teach granting a workstation access to a service prior to authenticating a user to access the service.

Application Serial No. 09/665,018

The McGraw Publication

The McGraw publication only describes authenticating a user to access a service and not granting a workstation access to a service irrespective of a user. As noted by the Examiner, the Greenfield reference refers the reader to the McGraw publication in column 7, lines 23-30 of the Greenfield reference. The McGraw publication is referred to by the Greenfield reference to provide more detailed information about Java sandbox technology.

Summary for Independent Claim 1

In light of the differences between amended independent Claim 1 and the Gaul, Greenfield, and McGraw references noted above, one of ordinary skill in the art recognizes that these prior art references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 1. Accordingly, reconsideration and withdrawal of the rejection of Claim 1 are respectfully requested.

Independent Claim 8

The rejection of Claim 8 is respectfully traversed. It is respectfully submitted that the Gaul, Greenfield, and McGraw references, fail to describe, teach, or suggest the combination of: (1) issuing a request for a scanner to a network server from a browser operating on the workstation; (2) transmitting the scanner and a workstation policy from the network server to the workstation via the computer network, the scanner installable within the browser and operative to generate workstation credentials by completing a vulnerability assessment of the workstation, the workstation credentials comprising at least one of information about integrity of the workstation and a security posture of the workstation; (3) comparing the workstation credentials to the workstation policy on the workstation to determine whether the workstation should be granted access to the software service; (4) granting the workstation access to the software service available on the network server if the workstation credentials are in compliance with the workstation policy; and (5) if access to the software service is granted to the workstation because the workstation credentials are in compliance with the workstation policy, issuing a request for user authentication in order to determine if a user of the workstation is authorized to

Application Serial No. 09/665,018

access the service available on the network server, as recited in amended independent Claim 8.

As noted above with respect to independent Claim 1, the Gaul and Greenfield references and the McGraw publication do not provide any teaching of granting access to a system or network for a workstation and then requesting further information about a user of the workstation in order to authenticate a user when the workstation has been granted access to the network.

In light of the differences between Claim 8 and the references mentioned above, one of ordinary skill in the art recognizes that the Gaul and Johnson references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in independent Claim 8. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 11

The rejection of Claim 11 is respectfully traversed. It is respectfully submitted that the Gaul, Greenfield, and McGraw references, fail to describe, teach, or suggest the combination of: (1) issuing a request for a scanner to the network server from a browser operating on the workstation; (2) transmitting the scanner from the network server to the workstation via the computer network, the scanner installable within the browser and operative to generate workstation credentials by completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network; (3) the workstation credentials comprising at least one of information about integrity of the workstation and a security posture of the workstation; (4) transmitting the workstation security credentials from the scanner to the network server via the computer network; (5) determining at the network server whether the workstation should be granted access to a network service of the network based on the workstation credentials; and (6) granting the workstation access to the network service if the workstation credentials are in compliance with the workstation policy; and (7) if access is granted to the workstation for the network service because the workstation credentials are in compliance with the workstation policy, issuing a request

Application Serial No. 09/665,018

for information relating to user authentication in order to determine if the user is authorized to access the network service, as recited in amended independent Claim 11.

As noted above with respect to independent Claim 1, the Gaul and Greenfield references nor the McGraw publication provide any teaching of granting access to a network service for a workstation and then requesting further information about a user of the workstation in order to authenticate a user to access the service when the workstation has already been granted access to the service.

In light of the differences between amended Claim 11 and the references mentioned above, one of ordinary skill in the art recognizes that the prior art references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 11. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Dependent Claims 2-7, 9-10, and 12-20

The Applicants respectfully submit that the above-identified dependent claims are allowable because the independent claims from which they depend are patentable over the cited references.

Dependent Claims 15-20 emphasize the difference between workstation credentials and credentials associated with a user. The workstation credentials are used to determine if a workstation should be allowed to proceed with authenticating a user. In this way, if the workstation credentials indicate that authentication of a user should not be allowed to proceed, then the authentication process is terminated before a user presents his or her credentials over the computer network.

The Applicants also respectfully submit that the recitations of all the dependent claims are of patentable significance. Accordingly, reconsideration and withdrawal of the rejections of the dependent claims are respectfully requested.

CONCLUSION

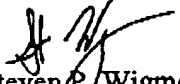
The foregoing is submitted as a full and complete response to the Office Action mailed on July 12, 2005. The Applicants and the undersigned thank Examiner Colin for the consideration of these remarks. The Applicants have submitted remarks to traverse

Application Serial No. 09/665,018

the rejections of Claims 1-20. The Applicants respectfully submit that the present application is in condition for allowance. Such Action is hereby courteously solicited.

If any issues remain that may be resolved by telephone, the Examiner is requested to call the undersigned at 404.572.2884.

Respectfully submitted,


Steven P. Wigmore
Reg. No. 40,447

October 12, 2005

King & Spalding
45th Floor
191 Peachtree Street, N.E.
Atlanta, Georgia 30303
404.572.4600
K&S Docket: 05456-105007